



Common Policy CP Change Proposal Number: 2010-07

To: Federal PKI Policy Authority
From: Certificate Policy Working Group
Subject: Proposed modifications to the Common Policy CP
Date: November 5, 2010
Title: Legacy use of SHA-1 during the transition period January 1, 2011 to December 31, 2013

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework Version 3647 – 1.12, October 15, 2010.

Organization requesting change: Federal PKI Certificate Policy Working Group

Change summary: This change proposal permits the continued use of SHA-1 to generate signatures on CRLs and OCSP responses that provide status information for certificates whose signatures were generated using SHA-1. It also introduces new certificate policy OIDs for certificates signed with SHA-1 on or after January 1, 2011.

Background: There are some applications in use within the federal government that cannot process certificates or certificate revocation information that was signed using SHA-256. This change proposal makes it possible for such applications to accept certificates that were signed before December 31, 2010, using SHA-1 by permitting the certificate status information for such certificates to also be signed using SHA-1.

In addition, certificates issued between January 1, 2011 and December 31, 2014 can be signed using SHA-1 if they assert certificate policy OIDs that identify the use of SHA-1.

Use of certificates asserting certificate policy OIDs that identify the use of SHA-1 under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.

Specific Changes:

Insertions are underlined, deletions are in ~~striketrough~~ text:

FOREWORD

Modify the first and fifth paragraphs of the Foreword and add a new paragraph 6 as follows:

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates six specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy. There are two Certification Authorities associated with the Common Policy Framework: The Federal Common Policy Root CA and the SHA-1 Federal Root CA.

For entities associated with the Federal Common Policy Root CA, this ~~This~~ policy framework requires the use of either 2048 bit RSA keys or 256 bit elliptic curve keys along with the SHA-256 and SHA-384 hash algorithms. CAs are required to use 2048 bit RSA keys or 256 bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2010. CAs are required to use SHA-256 or SHA-384 when signing certificates ~~and CRLs~~ that are issued after December 31, 2010. All subscriber signature keys in certificates that expire on or after December 31, 2008 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys. Subscriber authentication keys in certificates that expire on or after December 31, 2013 must be at least 2048 bit RSA keys or 256 bit elliptic curve keys.

For entities associated with the SHA-1 Federal Root CA, subscriber certificates may assert a certificate policy OID that indicates the use of SHA-1, if issued before December 31, 2013. CAs that issue SHA-1 certificates after December 31, 2013 may not also issue SHA-256 certificates.

1. INTRODUCTION

Add a new paragraph after the first paragraph in the introduction:

The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. However, there are some applications in use within the federal government that cannot process certificates or certificate revocation information signed using SHA-256. Therefore this CP also includes five additional distinct certificate policies which indicate the use of the deprecated SHA-1 after December 31, 2010. These id-fpki-sha1 policies adhere to all the requirements of the associated id-common policy with the exception that the certificate is generated with a SHA-1 signature and the issuing CA may use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013. It should be noted that certificates issued on or after January 1, 2011 are not FIPS 201 compliant, and therefore do not meet the requirements of HSPD-12. CAs that issue SHA-1 certificates after December 31, 2010 may not also issue FIPS 201 compliant certificates.

1.2 DOCUMENT NAME AND IDENTIFICATION

Modify the first paragraph of 1.2 and add a new table, captions to both tables and 2 additional paragraphs at the end:

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CA shall assert at least one of the following OIDs in the certificate policy extension:

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}

Additionally, this CP provides moderate assurance concerning identity of certificate subjects when the following OIDs are expressed in certificate policy extensions of certificates issued after December 31, 2010, associated with the SHA-1 Federal Root CA, and signed using SHA-1.

Table 2 - id-fpki-SHA1 Policy OIDs

<u>SHA1 Policy</u>	<u>OID</u>	<u>Corresponding id-fpki-common policy</u>
<u>id-fpki-SHA1-policy</u>	<u>::= {TBD}</u>	id-fpki-common-policy id-fpki-certpcy-mediumAssurance
<u>id-fpki-SHA1-hardware</u>	<u>::= {TBD}</u>	id-fpki-common-hardware id-fpki-certpcy-mediumHardware
<u>id-fpki-SHA1-devices</u>	<u>::= {TBD}</u>	id-fpki-common-devices id-fpki-certpcy-mediumAssurance
<u>id-fpki-SHA1-authentication</u>	<u>::= {TBD}</u>	id-fpki-common-authentication id-fpki-certpcy-mediumHardware
<u>id-fpki-SHA1-cardAuth</u>	<u>::= {TBD}</u>	id-fpki-common-cardAuth

The requirements associated with a id-fpki-SHA1 policy are identical to those defined for the corresponding id-fpki-common policy, except that the certificates asserting id-fpki-SHA1- policies are signed with SHA-1, and the issuing CAs can use SHA-1 for generation of PKI objects such as CRLs and OCSP responses until December 31, 2013.

1.3.1.3 FPKI Management Authority (FPKI MA)

Modify 1.3.1.3 as follows:

The FPKI Management Authority is the organization that operates and maintains the Common Policy Root CA and the SHA-1 Federal Root CA on behalf of the U.S. Government, subject to the direction of the FPKIPA. All of the requirements for the SHA1 Federal Root CA are identical to the Common Policy Root CA except that the SHA1 Federal Root CA asserts id-fpki-sha1 policies and shall use SHA-1 for generation of PKI objects such as certificates, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses after December 31, 2010 and before December 31 2013.

1.4.1 Appropriate Certificate Uses

Add new paragraph at end

The digital signatures on certificates issued under this policy may be generated using SHA-1 only when one or more of the id-fpki-SHA1 policy OIDs is used . The use of SHA-1 to create digital signatures is deprecated beginning January 1, 2011. As such, use of SHA1 certificates issued under this policy should be limited to applications for which the risks associated with the use of a deprecated cryptographic algorithm have been deemed acceptable.

6.1.5 Key Sizes

Modify the fourth and fifth paragraphs of Section 6.1.5 and add an additional paragraph as follows:

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-256, or SHA-384 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that are issued after December 31, 2010 shall be generated using SHA-256, however, RSA signatures on CRLs that are issued before January 1, 2012, and that include status information for certificates that were generated using SHA-1 may be generated using SHA-1. RSA signatures on CRLs that are issued on or after January 1, 2012, but before January 1, 2014 that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1. ECDSA signatures on certificates and CRLs ~~that expire on or after December 31, 2010~~ shall be generated using SHA-256 or SHA-384, as appropriate for the key length.

RSA signatures on certificates that are issued after December 31, 2010 and before January 1, 2014, to CAs that issued certificates prior to December 31, 2010 may be generated using SHA-1 provided that CA issues no additional end entity certificates. Additionally, certificates issued to OCSP responders that include SHA-1 certificates may be signed using SHA-1 until December 31, 2013. CAs that issue certificates signed with SHA 224 or SHA 256 after December 31, 2010 must not issue certificates signed with SHA 1.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs. After December 31, 2010, OCSP responders that generate signatures on OCSP responses using SHA-1 shall only provide signed responses that are pre-produced (i.e., any signed response that is provided to an OCSP client shall have been signed before the OCSP responder received the request from the client).

7.1.6 Certificate Policy Object Identifier

Modify 7.1.6 as follows:

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= { 2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware ::= { 2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices ::= { 2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication ::= { 2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High ::= { 2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth ::= { 2 16 840 1 101 3 2 1 3 17}

Certificates generated with SHA-1 after December 31, 2010 shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-SHA1-policy ::= { TBD }
id-fpki- SHA1-hardware ::= { TBD }
id-fpki- SHA1-devices ::= { TBD }
id-fpki- SHA1-authentication ::= { TBD }
id-fpki- SHA1-cardAuth ::= { TBD }

7.2 CRL PROFILE

Modify 7.2 as follows:

CRLs issued by a CA under ~~this~~ the id-fpki-SHA1-authentication, id-fpki-SHA1-cardAuth, or id-fpki-SHA1-hardware policy shall conform to the CRL profile specified in [CCP-PROF] except that SHA-1WithRSAEncryption may be used as the signature algorithm in CRLs that are issued before January 1, 2014.

Estimated Cost:

The FPKI MA will incur the costs for establishing the new parallel SHA1 Federal Root CA.

SSPs supporting Federal Agencies unable to transition to SHA-256 by January 1, 2011 may incur the costs for establishing one or more new SHA-1 parallel CAs.

Risk/Impact:

The use of SHA-1 to create digital signatures will be deprecated beginning on January 1, 2011, due to the risk of collision attacks. While this is a significant concern for certificates, where the applicant, who may be untrusted, may provide some of the information that will be placed in a certificate, this is less of a concern when all of the information to be signed is created by a trusted entity without input from any untrusted source. For this reason the risk of collision attacks against CRLs are considered to be less significant than for certificates. OCSP responders may either generate a fresh response for each OCSP request or may pre-produce signed responses and only provide these cached responses in response to OCSP requests. If the OCSP responder creates a fresh response for each request that is tailored to the request, then there is a risk that the untrusted client may have crafted the request in such a way as to create a collision in the response. If the OCSP responder only provides pre-produced signed responses, then this possibility is eliminated since the client's request cannot influence the contents of the signed response.

Federal agencies have identified critical applications that are unable to support the use of PKI objects generated with SHA-256 signatures by January 1, 2011. These organizations may determine the risk of continued use of the deprecated SHA-1 is outweighed by the known risk of disruption of services which will be caused by transitioning to SHA-256 at this time.

Implementation Date:

This change to the policy will be effective immediately upon approval by the FPKIPA and incorporation into the Common Policy CP.

Prerequisites for Adoption: None

Plan to Meet Prerequisites: N/A

Approval and Coordination Dates:

Date presented to CPWG: November 5, 2010

Date presented to FPKIPA: November 9, 2010

Date of approval by FPKIPA: TBD